



Release Notes

3Com® Router 5000 and 6000 Family

Software Version 2.41

Part Number: 10015046 rev. AC

Published Date: August 2007

Contents

1. Introduction	2
1.1 Scope.....	2
1.2 Online Resources.....	2
1.3 System Requirements	2
1.4 Support for New Modules in v2.41	3
1.5 Support for Previously-Released Modules in v2.41	3
2. Issues Fixed in Release v2.41	5
2.1 Software Issues Resolved Since v2.30/2.31	6
2.2 Software Issues Resolved from v2.11	6
2.3 Software Issues Resolved from v2.20.....	8
2.4 User Documentation Issues resolved From v2.20	8
2.5 Software Issues Resolved from v2.21	9
2.6 Documentation Issues Resolved since v2.21	9
3. Known Issues for Router 5000 and Router 6000 Release v2.41	9
3.1 System Access.....	9
3.2 SNMP.....	10
3.3 System Management	10
3.4 Interface Management.....	10
3.5 Link Layer Protocol	11
3.6 Network Protocol	12
3.7 Routing Protocol	12
3.8 Multicast Protocol	13
3.9 Security/VPN.....	13
3.10 Quality of Service (QoS).....	14
3.11 MPLS.....	14
3.12 Interoperability Issues between the Router 5000/Router 6000 and 3Com VCX V7000	14
3.13 Documentation Errors	16
4. Upgrading Software	16
4.1 Upgrading with FTP.....	16
4.2 BOOT Menu	17
4.3 Upgrading Software Using Xmodem	20
4.4 Upgrading Software Using TFTP (option 1)	21
4.5 Upgrading Software Using TFTP (option 2)	22

1. Introduction

1.1 Scope

These release notes summarize the operational requirements and known issues for the 3Com® Router 5000 and Router 6000 software releases listed Table 1. This release notes supersede the v2.20, v2.21, v2.30/2.31, and v2.40 Release Notes for the Router 5000 and Router 6000.

This release provides an update to the Router 5000 and Router 6000. The software for the Router 6000 RPU2 will not load on the Router 6000 RPU.

Table 1: Software Release v2.41

Software Release Filenames	Description
R6y02_41e.bin	The encrypted software agent which runs on the Router 6040 and 6080 RPU2 (including bootrom)
R6y02_41v.bin	The basic software agent which runs on the Router 6040 and 6080 RPU2 (including bootrom)
R6x02_41e.bin	The encrypted software agent which runs on the Router 6040 and 6080 RPU (including bootrom)
R6x02_41v.bin	The basic software agent which runs on the Router 6040 and 6080 RPU (including bootrom)
R5y02_41v.bin	The basic software agent which runs on the 5012, 5232, 5642, 5842 Routers
R5y02_41e.bin	The encrypted software agent which runs on the 5012, 5232, 5642, 5842 Routers
bootromfull9-17.bin	Router 5000 Boot ROM file for 5012, 5232, 5642, 5842 Routers

Table 2: Supported Routers

Router 5012 3-Slot (3C13701)	Router 6040 4-Slot (3C13840)
Router 5232 3-Slot (3C13751)	Router 6080 8-Slot (3C13880)
Router 5642 4-Slot (3C13755)	
Router 5682 8-Slot (3C13759)	

1.2 Online Resources

Visit the 3Com web site for the latest documentation and software updates: **www.3Com.com**

- Obtain a copy of the Router 5000 or Router 6000 *Installation Guide*, *Command Reference Guide*, or *Configuration Guide*.
- Obtain current software updates (maintenance releases) and associated release notes for the Router 5000 and Router 6000 and other 3Com products.

1.3 System Requirements

The Router 5000 and Router 6000 have these minimum requirements for successful operation:

- Router 6040 or Router 6080 Chassis

- Power Supply
- Router 6000 RPU2 with flash memory minimum 64 Mb
- Loadable software image (includes bootrom)
- Modules as needed

1.4 Support for New Modules in v2.41

Table 3: Additional New Modules Supported in Release v2.41

Product #	Description
3C13805	Router 6000 RPU2
3CR13806-75	Router 6000 RPU2 Encryption Accelerator
3CR13873-75	Router NDEC2 Encryption Accelerator FIC
3C13715	Router 1-Port Enhanced Serial SIC
3C13775A	Router 1-Port FT3/CT3 MIM
3C13877A	Router 1-Port T3 ATM FIC
3C13879	Router 1-Port GbE Fiber FIC
3C13881A	Router 1-Port OC3 POS FIC
3C13882A	Router 1-Port OC3 ATM MM FIC
3C13884A	Router 1-Port OC3 ATM SM FIC
3C13886A	Router 1-Port OC3 ATM SML FIC
3C13889A	Router FT3/CT3 FIC
3C13890	Router 2-Port FXS FIC
3C13891	Router 4-Port FXS FIC
3C13893	Router 2-Port FXO FIC
3C13894	Router 4-Port FXO FIC
3C13895	Router 2-Port E&M FIC
3C13896	Router 4-Port E&M FIC
3C13897	Router 1-Port E1 Voice FIC
3C13898	Router 1-Port T1 Voice FIC

1.5 Support for Previously-Released Modules in v2.41

Table 4: Previously Released Modules Supported by v2.41

Product #	Label
MIMs (Multifunction Interface Modules; Router 5000 Family)	
3C13761	Router 2-Port 10/100 MIM
3C13762	Router 2-Port Enhanced Serial MIM
3C13763	Router 4-Port Serial MIM
3C13764	Router 4-Port Enhanced Serial MIM

3C13765	Router 2-Port CE1/PRI MIM
3C13766	Router 4-Port CE1/PRI MIM
3C13767	Router 4-Port ISDN-S/T MIM
3C13769A	Router 2-Port CT1/PRI MIM
3C13770	Router 1-Port ADSL over POTS MIM
3C13771-75	Router NDEC Encryption Accelerator MIM
3C13772	Router 2-Port ADSL over POTS MIM
3C13774	Router 1-Port 10/100/1000 MIM
3C13775A	Router 1-Port CT-3 MIM
3C13777	Router 1-Port CE3 MIM
3C13778	Router 4-Port E1-IMA (120 Ohm) MIM
3C13779	Router 4-Port T1-IMA MIM
3C13780	Router 2-Port FXS MIM
3C13781	Router 4-Port FXS MIM
3C13783	Router 2-Port FXO MIM
3C13784	Router 4-Port FXO MIM
3C13785	Router 2-Port E&M MIM
3C13786	Router 4-Port E&M MIM
3C13787	Router 1-port E1 Voice MIM
3C13788	Router 1-port T1 Voice MIM
3CR13773-75	Router NDEC2 Encryption Accelerator MIM
SICs (Smart Interface Cards; Router 5000 Family)	
3C13712	Router 1-Port 10/100 SIC
3C13714	Router 1-Port Serial SIC
3C13715	Router 1-Port SAE SIC
3C13716	Router 2-Port ISDN-S/T SIC
3C13718	Router 2-Port ISDN-U SIC
3C13720A	Router 1-Port Fractional T1 SIC
3C13722	Router 1-Port Fractional E1 SIC
3C13724	Router 1-Port Analog Modem SIC
3C13725	Router 1-Port FXS SIC
3C13726	Router 2-Port FXS SIC
3C13727	Router 1-Port FXO SIC
3C13728	Router 2-Port FXO SIC
FICs (Flexible Interface Cards; Router 6000 Family)	

3C13821	Router 4-Port Fractional T1 FIC
3C13821A	Router 4-Port Fractional T1 FIC
3C13823	Router 4-Port Fractional E1 FIC
3C13860	Router 1-Port 100FX MM FIC
3C13861	Router 2-Port 10BASE-T/100BASE-TX FIC
3C13862	Router 1-Port 100FX SM FIC
3C13863	Router 4-Port Enhanced Serial FIC
3C13864	Router 8-Port Enhanced Serial FIC
3C13866	Router 4-Port E1/ Channelized E1/PRI FIC
3C13870A	Router 4-Port T1/ Channelized T1/PRI FIC
3C13871	Router 1-Port ADSL over POTS FIC
3C13872	Router 2-Port ADSL over POTS FIC
3C13874	Router 4-Port E1-IMA (120 ohm) FIC
3C13875	Router 4-Port T1-IMA FIC
3C13876	Router 1-Port E3 ATM FIC
3C13887	Router 1-Port 10BASE-T/100BASE-TX/1000BASE-T
3C13888	Router 1-Port E3/ Channelized E3 FIC
3C13890	Router 2-Port FXS FIC
3C13891	Router 4-Port FXS FIC
3C13893	Router 2-Port FXO FIC
3C13894	Router 4-Port FXO FIC
3C13895	Router 2-Port E&M FIC
3C13896	Router 4-Port E&M FIC
3C13897	Router 1-Port E1 Voice FIC
3C13898	Router 1-Port T1 Voice FIC
3CR13873-75	Router NDEC2 Encryption Accelerator FIC
3CSFP71	OC3 SM (15km) SFP Transceiver
3CSFP81	OC3 MM & 100BASE-FX SFP Transceiver
3CSFP91	1000BASE-SX SFP Transceiver
3CSFP92	1000BASE-LX SFP Transceiver
3CSFP93	1000BASE-T SFP Transceiver
3CSFP97	1000BASE-LH SFP Transceiver

2. Issues Fixed in Release v2.41

This section describes issues that have been resolved since previous releases of the software.

2.1 Software Issues Resolved Since v2.30/2.31

The following issues have been resolved since the v2.30/2.31 release of this software.

- VCX calls fail across a NAT network.
- NBX phones fail to load across a NAT network.
- IPX is now supported on Frame Relay, Ethernet and PPP. IPX is not supported on, HDLC, and X25.
- When setting the main/backup images, the file pointer does not point to flash:/ by default; the flash device must be included in the path; for example, bootfile main flash:/main.bin rather than just bootfile main main.bin.
- When there is a high traffic load on the router, and the CLI response time slows, the CPU usage information is not accurately displayed.
- Gigabit Ethernet and POS interfaces do not support auto-install.
- SYS MGMT — Router 5000 series routers report that the system returned to service via “power-on” even if the router is warm booted.
- IPSEC policy with a deny rule before a more general permit rule will not enforce the deny rule.
- Resetting the IKE SA does not reset the tunnel completely; Resetting both sides at the same time is currently required to completely reset the tunnel.
- IPSec tunnel resets (resetting IKE SA/IPSec SA) may result in router reboot.
- CBR traffic approaching PCR on a PVC will experience packet loss when UBR traffic on a separate PVC is introduced on the ATM link
- Service classes on IMA group interfaces have cell rate limits of just one T1/E1 Link regardless of how many links are in the bundle.

2.2 Software Issues Resolved from v2.11

The following issues have been resolved since the v2.11 release of this software.

- In some specific circumstances, displaying virtual-access on a router with MLPPP may cause a reboot. To resolve this, use the command, Display Virtual Template instead.
- A virtual baud rate setting of 786000 is not available on a serial interface.
- The state of Promiscuous mode on an Ethernet interface is not shown in the “display current” command. To view the state of Promiscuous mode, use the “display interface Ethernet x/x” command.
- Gigabit Ethernet interfaces will not forward traffic if they are assigned to a bridge-set. Gigabit interfaces should only be assigned to routed interfaces.
- When a bridge-set is removed from an Ethernet interface the message “Promiscuous operation mode was removed automatically” is displayed. However, promiscuous mode may not have been disabled on that interface. Manually verify that Promiscuous mode has been reset using the “display interface Ethernet x/x” command. If it has not been disabled, use the “undo promiscuous” command in the interface view.
- There is no support for ISDN switch type DMS100.
- Frame Relay sub-interface definition types (P2MP, P2P) are not displayed. To determine the interface type, display the interface as follows: “Display fr pvc interface <interface> <dlci>.”

- Frame Relay Classes that contain Frame Relay QoS parameters can be applied to PVCs even though Frame Relay Traffic Shaping is not enabled. Frame Relay Traffic Shaping must be enabled for PVC queues to be functional.
- When IPsec policies are configured on both the incoming and outgoing interfaces, one of the interfaces needs to have IPsec over GRE configured to allow multicast IP fragments to pass through the router without problems.
- The ability to add inline comments to describe an ACL as a whole is available, however the ability to add a specific description to a rule is not available. Example: if an ACL is long and complicated, inline comments for the rule cannot be added. Save the current configuration and then edit in descriptive comments to that configuration.
- FDL and remote loop back issues.
- B8ZS and ESF issues.
- LBO range issues.
- Alarm Threshold Settings issues.
- Issues with viewing current alarms and error registers.
- Various issues with local, payload, and remote loopbacks.
- DEBUG commands on the serial interface and physical layer characteristics of the router modules.
- UNDO of the DEBUG function.
- Constant DEBUG output issues on the FT1 SIC module.
- No indication of resetting (zeroing) traffic statistics.
- Lack of input and output rates displayed in bits per second as part of traffic statistics output.
- A logging error where VPN information is logged erroneously, when there was no actual VPN configuration.
- Only one system user at a time able to access the console.
- With the display interface command, packet flow shows double that of the Ethernet interfaces.
- Inaccurate display information with ACL statistics, not properly incrementing for permit statements.
- Frame Relay statistics discrepancies on the sub-interface packet counts.
- Statistics on the FT1 and T1 interfaces not properly zeroed upon reset command, "reset counter interface".
- Banner information is lost upon FTP or TFTP while obtaining router information.
- A packet loss problem with small packet sizes configured.
- No display of trap settings with status.
- NAT traversal is not compatible with Cisco routers. IPsec tunnel is not established with Cisco routers when a NAT device is in the path.
- Only one security association is used for all traffic flows. IPsec SA is not flow based. IPsec SAs originated from 3COM routers will be ACL based. To obtain flow-based functionality, create multiple ACLs with one rule each.

2.3 Software Issues Resolved from v2.20

The following issues have been resolved since the v2.20 release of this software.

- Changing the speed and duplex on the Gigabit Ethernet Module does not take effect without resetting the interface manually. A manual “shutdown” and then “undo shutdown” is required to have the changes take effect.
- Loopback LED remains lit solid after remote side sends the loop down code. No Loopback LED indicator
- Banners edited offline in the proper format will be discarded when loaded into the system via ftp/tftp
- D4, D4/AMI and ones density are not supported.
- FDL AT&T payload option issues.
- No fdl-att-plb-up and fdl-att-plb-down are available.
- Alarm LED — No Alarm LED indicator
- BERT issues — Bits received since test started and Bits received since latest sync do not match on a perfect loop
- NAT display issues — NAT sessions do not display “NO-PAT”

2.4 User Documentation Issues resolved From v2.20

The following user Documentation issues have been resolved since the v2.20 release of this software.

- ACL numbering scheme is different from those documented in the Command Reference Manual. Use the following corrected numbering scheme:
 1000-1099 (Interface-based ACL)
 2000-2099 (Basic ACL)
 3000-3099 (Advanced ACL)
 4000-4999 (Ethernet Frame Header ACL)
- The Command Reference manual states that “reset ike sa” will clear both phase 1 and phase 2 security associations. “Reset ike sa” will only clear phase 1 security associations; “reset ipsec sa” will clear phase 2 security associations.
- MPLS LDP loop detect cannot be configured after LDP is enabled on interface. An error is reported. Enable LDP loop detect under system view before enabling LDP on the interface.
- The “virtualbaudrate” command is non-existent in the Command Index. Use the “virtualbaudrate” command in the Command Line Interface (CLI).

```
[xxxx-3-Serial2/0/4]virtualbaudrate?
300      only for async mode
600      only for async mode
1200     for syn & asyn mode
2400     for syn & asyn mode
4800     for syn & asyn mode
9600     for syn & asyn mode
19200    for syn & asyn mode
38400    for syn & asyn mode
56000    only for syn mode
57600    for syn & asyn mode
64000    only for syn mode
72000    only for syn mode
```


115200	for syn & asyn mode
128000	only for syn mode
384000	only for syn mode
2048000	only for syn mode

2.5 Software Issues Resolved from v2.21

The following issues have been resolved since the last release, v2.21, of this software.

- If the user cut and pastes within the BootRom menu to fill in fields (such as filenames for TFTP downloads) the display will only show a maximum of 8 characters. If the filename is longer it will be accepted by the system, but will not display characters beyond the initial 8.
- The “more” command truncates large config files(>17KB) on the 5012 routers. If the file needing to be read is not the saved configuration, transfer the file to a PC disk, and read it from there. If it is the saved configuration, read it with the “display saved-configuration” command.
- Display ft1 will display the same statistics multiple times, once for each Frame Relay interface/sub-interface configured.
- The current IMA aggregate baud rate does not change when links are added or removed, when using the display interface command. This is a display problem only.
- The Gigabit Ethernet module does not support half duplex mode at 100 Mb setting.
- Display fr pvc statistics do not account for the outbound packets.
- The bridge <x> mac-address command for setting a static MAC entry for a gigabit Ethernet interface is not supported.
- The bridge <x> mac-address <xxxx-xxxx-xxxx> permit interface command is not an option for a Gigabit type interface. This command is not supported for Gigabit interfaces.
- CRC and PAD errors on the 1-Port ADSL Module interfere with even the lowest traffic loads, of expected normal operation — Example 256K traffic on 8Mb link.
- PIM is not supported over an IPsec tunnel. PIM hellos are rejected over an IPsec Tunnel.
- The first IKE peer with local-address defined will have its address be used for all IKE peers in the policy.
- ATM VBR service classes will fail to be set at Peak Cell Rates higher than 124492 kbps (for OC3-ATM), 41923 kbps (for T3-ATM) and 33340 kbps (for E3-ATM).

2.6 Documentation Issues Resolved since v2.21

User Documentation issues resolved since the last release, v2.21, of this software.

- Named access list is documented but not supported.
- Name based ACLs, as listed in the command reference manual, are not supported.

3. Known Issues for Router 5000 and Router 6000 Release v2.41

3.1 System Access

- The router does not allow configuring of an FTP server with Radius Authentication None option. FTP Anonymous login is not supported. A username and password is required for FTP access.
- The FTP server does not support filenames containing spaces. 3Com recommends using underscores instead of spaces as separation delimiters.

- To get ftp inputs to work properly from a client, ftp update normal must be set on the router.

3.2 SNMP

- The router does not respond to SNMP when the user is logged into the System View. This causes Network Management Systems such as 3Com Router Manager and 3Com Network Director to generate errors. To resolve this, exit the System View.
- The Frame Relay MIB does not use the latest version of the RFC 2115. As a result, public MIB variables for troubleshooting Frame Relay performance problems are not supported; (e.g. frCircuitLogicalIndex) from the current FRAME_RELAY-DTE-MIB (RFC 2115)
- The router will send an initial invalid trap packet upon link down/up event, followed by the correct Trap packet. Ignore the first trap packet, the second packet is correct.

3.3 System Management

- On RPU2s when booting from the compact flash, it is possible to get the following error on boot up: "Error encountered during checking disk, format the disk!" and the boot will not complete. Power down the router and power it back up to clear the problem.
- Analog Modem debugging shows internal activity when no cable is connected. This indicates that the modem is active and ready to receive or make calls.
- When saving a configuration to a non-existing directory the following message displays: "Cannot open the configuration file, this may be caused by insufficient memory space". This is an incorrect message and is displayed when the user is trying to save a file to a non-existent directory. To solve the problem, create the directory first.
- When rebooting the router, the Current Configuration change detection sometimes detects changes when there were none, and a warning message is displayed.
- There is no way to recover if both the Bootrom password and the console password are lost. If both passwords are lost, the router must be returned to 3Com for repair (RMA).
- FTP user cannot be cleared; set the ftp time-out to 1 minute to clear an inactive session rather than waiting the 30 minutes set by default.
- The display current-configuration command with a filter will not recognize the underscore character("_") alone. Use the backslash character("\") in front of the underscore to get the desired result. For example, display current-configuration | begin bgp_peer will display the configuration starting with the line containing "bgp_peer"
- CPU Usage history graph has the time scale backwards; the right side is the most recent history.
- A 1-Port Channelized E3 MIM card will not operate if inserted in slot 0 on the 5642 or slot 1 on the 5232. Select a different slot for the E3.

3.4 Interface Management

- When the Dialer interfaces toggles state (up or down), minor packet loss will occur for any packet passing through the router.
- Interface statistics with a flow-interval of under 10 seconds are not accurate. Do not enter flow- interval values under 10 seconds.
- The Virtual-Ethernet interface protocol state displays as being down when running PPPoE. This is the normal operating state of the Virtual-Ethernet interface.

- On an ISDN interface, the Line Protocol state is up when no cable is attached to the port on the interface. It is best to observe the interface's Current State. The Current State will be down if no cable is attached to the interface even though the Line Protocol will show it as up.
- A Frame Relay sub-interface that has been configured as "Down" transmits packets.
- Displaying a Fractional E1 interface displays a Frame Format equal to NONE. The actual Frame Format is no-crc.
- Frame Relay Payload Compression is displayed for PVC even after it is removed. Reset the interface to resolve.
- Display interface for an ATM interface with sub-interfaces will display the same cumulative statistical information - no individual statistics are provided; Instead use, display atm interface to show more individualized statistics.
- An ATM PVC that is set with rate limiting and is heavily oversubscribed with data, will fail to pass traffic. Other PVCs continue to work on the link.
- Changing the speed on a modem interface resets the interface. Do not change the modem interface speed while a dialup session is active.
- The activity LED on the T3 ATM Module indicates heavy activity regardless of the amount of traffic passing through it.
- Regardless of actual traffic running or not, T3 and E3 activity LEDs blink constantly.

3.5 Link Layer Protocol

- A frame relay link will not come up if the IP Address is changed, because the fr inarp table is not refreshed. The user must reset the fr inarp table manually.
- Alarm-threshold values are not configurable when a T1-line is configured within a T3 link.
- Level-4 alarm-threshold is not supported for T1 links setup for SF frame format. The CLI will not report an error.
- ATM AIS/RDI statistics are inaccurate.
- ATM OAM Segment Loop cells are not supported.
- Frame Relay PVCs can be modified when they are part of a PVC switching endpoint. Verify first that the interface is not a PVC endpoint before making any changes, else traffic may be disrupted.
- There is no DEBUG support for Multilink Fragmentation (FRF.16.1).
- Status and statistics for Multilink Fragmentation (FRF.16.1) cannot be viewed
- There is no support for ISDN switch type AT&T for BRI U interfaces. The router Command Line Interface and the documentation specifically states that AT&T is only supported on PRI interfaces. The default isdn protocol-type dss1 will connect to switches using AT&T switch type on a BRI interface. This was tested with Lucent 5E, otherwise known as AT&T 5ess.
- Bridge-set traffic cannot be routed even though a bridge-set can be configured with an IP address.
- FRF.9 Compression is still displayed upon viewing of PVC statistics, after the PVC is re-mapped without FRF.9. After re-mapping a PVC to exclude FRF.9 compression, reset the interface in order to clear any reference to FRF.9

- When removing FRF.9 compression settings from a frame relay static address mapping, the interface needs to be reset (shutdown/undo shutdown) for the configuration to take place.
- When the ATM OAM and PVC states are all down, the ATM interface is still showing state:UP and Line:UP; Use "display atm pvc-info" to see the true state of the individual PVCs.
- ATM statistics may be wrong if the traffic rate exceeds the Class of Service settings configured.
- PPP STAC compression is not supported on the POS interface.
- ATM OAM up/down timers for transitioning the PVC State are not accurate.
- ATM T3/E3 Modules require all cables to be connected before link LEDs will be lit.
- Changing MLPPP parameters will not take effect until the Virtual-Template or Mp-group is reset via bringing down all the physical interfaces and bringing them back up again.

3.6 Network Protocol

- Basic NAT doesn't work on R6080/R6040.
- PPP, Frame relay, HDLC, and E1 interfaces do not support DHCP Global subaddress mode.
- Certain web sites cannot be accessed when using DSL interfaces. To resolve this, set the outgoing router (WAN) physical or virtual interface to 1410 as the maximum segment size for TCP.
- The DHCP Server does not remember the DHCP clients after a reboot. The DHCP lease expiration, client reboot or client renew request will repopulate the DHCP clients table transparent to the user.
- A Router running DHCP client cannot obtain the default gateway address automatically. This parameter must be manually configured.
- ICMP type 3 messages are generated for some but not all instances in RFC 1812 (Section 5.2.7.1).

3.7 Routing Protocol

- Where Static Routes point to Ethernet interfaces, ARP responses are ignored. The next-hop must be specified for static routes on Ethernet interfaces.
- When BGP changes states, minor packet loss will occur at the instance of the change, for any packet passing through the router.
- OSPF interface costs are not the same on peer DCE/ DTE Frame Relay Serial interfaces. If a Frame Relay DTE Serial interface is configured for OSPF, and the DCE has a differing baud rate, the interface has to be configured with the "virtualbaudrate" command. Configure this command using the same baud rate as the DCE. After configuring, shut down and restart the interface.
- Undo RIP from interface view removes RIP globally. To remove RIP from interface view use the command, "Undo RIP work."
- BGP route dampening does not work for IBGP routes. BGP dampening is designed to work only for EBGP routes
- The 3Com router will not exchange RIP Updates with various 3rd Party vendor's equipment when MD5 "usual" implementation is configured. The 3Com router will only exchange RIP Updates with a 3rd Party vendor's equipment when MD5 "Non-Standard" implementation is configured. Use "Usual" to exchange RIP Updates between 3Com routers.

- The BGP route is not advertised if the IGP route is present in the forwarding table. Import the route into BGP from the protocol which owns the route in the forwarding table.
- RIP Poison Reverse is not supported.
- IPX is not supported on HDLC and X25. IPX is only supported on Frame Relay, Ethernet, and PPP.
- The BGP received and advertised routes for a particular peer (display bgp routing-table peer <x.x.x.x> received|advertised) are not displayed in numerical order.
- With OAM and PVC states both down, the interface is still considered up and the directly connected route is not withdrawn from the routing table; Along the same line, with OAM active, a PVC's going down does not have its learned routes deleted from the routing table. The router will need to rely on the individual routing protocol's timeout feature to initiate route removal.
- Load Sharing statistics are not accurate when more than one next-hop router is reachable via the same physical interface.
- BGP Auto-summary does not work with the BGP Network command; Auto-Summary works in all other cases.
- Redistribution of IGP routes into IBGP will not have the IGP next-hop. Instead, the next hop will always be the router doing the redistribution.

3.8 Multicast Protocol

- The default value for the IGMP query interval (60 seconds) does not match the recommended value in RFC 2236 (125 seconds). Set the query interval to match the query interval of other routers in the network.
- PIM is not supported with IP unnumbered FR interfaces. An IP address must be assigned to the FR interface.
- The router will continuously reboot if the MSDP configuration references an interface that is not available; this would most likely occur when a module is removed or replaced and the saved configuration still has a reference to the old interface.

3.9 Security/VPN

- IPSec card-proposal does not have an option for ESP encapsulation. Those options do not show up until the "use" command is issued to specify which encryption module to use.
- The encryption card does not perform as well when passing large byte data(e.g. anything over 1464 bytes for 3DES/SHA1).
- "Display firewall ethernet-frame-filter all" does not work. Specify the exact interface to get the desired information.
- NAT traversal does not work in IKE Main Mode. IKE Aggressive Mode is required for NAT traversal to function properly.
- Packets with internal addresses appear outside the NAT boundary. NAT does not translate ESP or IGMP packets. NAT does not translate any IP protocols other than ICMP, TCP, UDP, and GRE (with respect to PPTP)
- The firewall drops FTP connections when ASPF is configured to filter TCP. ASPF must be configured with TCP and FTP together.

- With CRL checking enabled by default, certificate enrollment cannot be performed and an IPsec tunnel cannot be established without the CRL on the router. CRL checking must be disabled for certificate enrollment and the IPsec tunnel if the CRL is not on the router.
- If an undefined ACL is used in a configuration, a warning message is not displayed.
- In X.509 the CRL URL format determines which protocol is used to retrieve CRL from the CA server. Use one of the following CLI commands depending on specific Server support:

HTTP: `crl url http://<CA Server IP>/<CRL DP>`

LDAP: `crl url ldap://<CA Server IP>/<CRL DP>`

SCEP: `crl url "scep"`

- ACL matches for IPsec only count the first packet used to open the tunnel - subsequent packets will be logged in the IPsec SA.
- Manual Ipsec only protects the first match in an ACL with multiple rules; Recommendation: make only one rule per ACL to protect all desired traffic.
- IPsec transform negotiation is not compatible with Cisco; configure only one transform for any policy interacting with a Cisco router.
- IKE Keepalive is not accepted by a Cisco router and tears down the tunnel. Do not use the `ike sa keepalive-timer timeout` command (default).
- Juniper's IPsec implementation does not interoperate with the 3Com Router 5000 Family with respect to IPsec Fragmentation. If possible, set the MTU to 1438 or lower on devices that will be using the tunnel to avoid having to fragment IPsec packets.

3.10 Quality of Service (QoS)

- CBR miscalculates the remaining Bandwidth available after multiple PVCs oversubscribe the link. An "undo service" will recover all but 32kbps of the available bandwidth. A router reboot will recover the rest.
- QoS CBQ can be configured on a dialer interface but it has no effect. Place the QoS Policy on the physical interface rather than the logical dialer interface.
- Once a QoS policy is applied use the CLI command "reset IP Fast Cache" to re-apply the QoS functions properly.
- An under provisioned ATM service class results in link failure for that PVC only.

3.11 MPLS

- If there is no response, from pinging a CE Router from a PE Router within an MPLS/BGP L3 network use the command "ping -vpn -a xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx", using the source address of the PE interface that is in the VPN of the intended target.
- If Loopback0 and LSR ID ip addresses are different, MPLS LDP will not work properly. The Loopback0 and LSR ID ip addresses must be match.

3.12 Interoperability Issues between the Router 5000/Router 6000 and 3Com VCX V7000

- SIP compatibility mode is required for calls between 3Com Convergence Center Clients to router 5000/6000 analog phones. Execute the "sip-comp server" command from the voice view on the router.

- 3Com VCX 7000 phones do not support SIP outbound mode. DTMF digits sent from router 5000/6000 to VCX phones will be disregarded.
- Removal of the Master SIP server from a voice configuration will remove the following from the configuration:
 - Slave SIP server if one exists
 - “address sip proxy” for SIP VoIP entities
- Voice is barely audible when an NBX T1 is attached to the router configured running QSIG master (network side). Voice quality is poor over a T1 link when the T1VI module is configured for QSIG master (configured for ISDN network side.). QSIG master functions correctly over E1 using the E1VI module.
- The “select-rule type-first” command under the voice/dial view includes an option for VoFR. VoFR is not supported in this release. Make it the last choice in the select list.
- The “undo” command does not work for the mode command in the “controller/cas” view. To reset the mode to the default value use the “mode itu-t” command.
- By default, voice entities with the same match criteria are chosen at random. To prioritize VOIP entities use the command “select-rule type-first 213” command in the “voice/dial” view.
- Voice activity detection (VAD) is only supported when the G.723 codec is used.
- CAS is not supported on the T1VI module.
- RADIUS authentication and accounting is not supported for H.323.
- Only voice traffic is supported on E1 and T1 voice cards. This applies to Router 5000 & 6000 platforms. Data traffic is not supported over Router 5000 and 6000 Voice cards.
- FIC Voice Cards are not hot-swappable; these cards must be inserted/removed with the power off.
- A short static noise at the tail-end of the audio transmission is experienced when calls are placed across Router 5000 and Router 6000 FXS cards.
- The steps to bind the voice MAX-CALL function to a voice entity described in the user guide, is not clear. When configuring voice MAX-CALL you must apply this function inside the voice entity view.
- FXS ports do not support modem operations.
- All busy signals on voice cards are the same type: fast-busy signal.
- One-Stage dialing through POTS may take up to 5 rings before rings are heard on the remote side. Local ringing occurs before the remote side actually hears the rings.
- While accessing an outside line (two-stage dialing) the second dial tone takes a little longer than normal to be heard; wait for the second dial tone before proceeding.
- Caller-ID Name is not supported; the router does not generate the names tied to a local phone line.
- Analog voice quality is will be reduced when using analog lines across three or more routers.
- The user’s call forwarding option is not retained after a router reboot; the user must reprogram the call forwarding option after a router reboot to ensure proper forwarding operation.

- The router cannot detect when its own E&M, FXO/FXS, or E1 CAS E&M connections are down. Therefore, if a voice entity using one of these interfaces is routing calls, and the interface goes down, the router will not check for a voice entity with equivalent match criteria to use. The router will continue to attempt to send calls through the down interface.
- CLI doesn't support pre-defined ringing tones for the following countries: Colombia, EU, Egypt, Dubai, South Africa, and Australia.

3.13 Documentation Errors

- Bridging over Frame Relay is not listed as being supported in the "Router 5000-6000 Configuration Guide". Bridging over Frame Relay is supported.
- Spanning Tree is listed as not supported in "Router 5000-6000 Configuration Guide". Spanning Tree is supported.
- DVPN service is not enabled by default as stated in the user documentation. The user must enable it if needed.
- Firewall ASPF UDP detection does not support the following UDP based applications: TFTP, SSH, DHCP
- Ike peer-name does not seem to work as documented in the NAT-Traversal Example; In order to get name authentication to work, both sides must have id-type name configured. Both sides must have remote-names configured, and one side must have remote-ip configured (the initiator).
- The documentation incorrectly states that a VLAN port link type can be set to access, hybrid, or trunk. The Router 5000 and Router 6000 can only create trunk-type links by default, and the type cannot be changed.

4. Upgrading Software

This section describes how to upgrade the software in your 3Com Router.

4.1 Upgrading with FTP

Use the following procedure to upgrade the software with FTP:

- You must have level 3 privileges.
- 1 In the User View, enter: ftp <server ip address or hostname>.
 - a. Login to the server.
 - b. Set the transfer mode to binary.
 - c. Use the "get" command to download the new image.
 - d. Exit ftp.
 - 2 Enter the System View.
 - 3 Set the router to boot from the new image using "boot main <filename>".
 - 4 Exit the System View.
 - 5 Reboot the router.

The following example illustrates this procedure:

```
<6040>ftp 172.16.1.254
Trying 172.16.1.254 ... Press CTRL+K to abort Connected to 172.16.1.254.
220 181NAT Microsoft FTP Service (Version 5.0).
User(172.16.1.254:(none)):anonymous
```



```

331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
[ftp]binary
200 Type set to I.
[ftp]get r6y02_4lvc03.bin
200 PORT command successful.
150 Opening BINARY mode data connection for r6y02_4lvc03.bin(12693988
bytes).
.....226
Transfer complete.
FTP: 12693988 byte(s) received in 64.698 second(s) 196.00K byte(s)/sec.
[ftp]quit
221
<6040>sys
System View: return to User View with Ctrl+Z.
[6040]boot main flash:/r6y02_4lvc03.bin
Set main boot file successfully!
[6040]quit
<6040>reboot

```

4.2 BOOT Menu

- 1 Start the router, When "Press Ctrl-B to enter Boot Menu" appears, press <Ctrl+B>, you will be prompted to enter the Boot ROM password:

Please input bootrom password:

- 2 Once the correct password is entered (there is no password by default), the Boot menu is displayed, as shown below: (Note that the menu may be slightly different depending on the version of code used)

```

Boot Menu:
1: Download application program with XMODEM
2: Download application program with NET
3: Set application file type
4: Display applications in Flash
5: Clear configuration
6: Clear application password
7: Start up and ignore configuration
8: Enter debugging environment
9: Boot Rom Operation Menu
a: Do not check the version of the software b: Exit and reboot
Enter your choice(1-b):

```

Options of Boot menu are described in the following sections.

- 1: Download application program with Xmodem. (see Section 4.3)
- 2: Download application program with Ethernet. (see Section 4.5)

4.2.1 Boot Menu 3: Set application file type

Routers with more than 8 Mb of Flash provide a dual-image function. The system defines three default application files for booting the router (see below). When these files are loaded to Flash, the file specified by this option is used to boot the router. If you want to change the order or the boot file, you can select this option from the Boot ROM menu and make modifications.

The default names, types, and selected sequence of main, backup, and secure application files are described as follows:

- Main application file: default name is main.bin, file type M. This is the default file the system uses to boot.
- Backup application file: default name is backup.bin, file type B. This file will be used to boot system when the main file fails.
- Secure application file: default name is secure.bin, file type S. This file will be used to boot the router when the main and backup file fails. The system will display a booting failure message if the secure application file also fails.

Note:

- *Only the application file types M, B, and S can be used to boot the system. Applications marked as N/A cannot be used to boot the router.*
- *The names of the applications in Flash can be modified using CLI commands after the router has started. Refer to the "System Management" document for more information on the CLI commands. The application file types M, B, and N/A can be modified in either the Boot ROM menu or by the CLI commands after the application is started. Modifications to the file type of applications with type S are not allowed.*
- *Because the secure boot file is the last file the system uses to boot properly, the file type of secure boot file is not allowed to be changed, nor is it derived from any other type of file. It can only be downloaded via the Boot ROM menu, and its name must be specified as secure.bin. If you change the file name of the secure file using rename command after the system has started, there is no secure boot file in Flash and you need to download it again.*
- *Only one file of each type (M, B, and S) can exist in Flash. For example, if a file of type M and a file of type B exist in Flash, it is impossible to have a second file type of M or B. If the file type of another application is to be changed to B, the existing file of type B will be changed to N/A.*

When you select option 3 in the Boot ROM menu, the following menu appears (suppose there are four application files stored in Flash, all of which with following types:)

```

M=MAIN      B=BACKUP      S=SECURE
*****
NO.   Name           Size           Type           Time
1     main.bin       5988025        M              Oct/10/2002 10:10:10
2     backup.bin     5985198        B              Oct/10/2002 10:10:10
3     a.bin          987491         N/              Oct/10/2002 10:10:10
4     secure.bin     5988022        S              Oct/10/2002 10:10:10
*****
5     Exit to main menu

Enter your choice(1-5):    3

```

The following menu appears if you select 3, through which you can change the file type of a.bin.

```

Set this file as:
1. Main
2. Backup
3. Exit
Enter your choice(1-3):    1

```

If you select 1, a.bin will be specified as the main boot file. When the modification is validated, the type of the original main file is changed to N/A., and a.bin will be used to boot the router.

4.2.2 Boot Menu 4: Display applications in Flash

This option is to display the existing applications (and their types) in Flash. The following information appears when you select option 4 in the Boot ROM menu (suppose that the above modification is validated).

```

      M=MAIN      B=BACKUP      S=SECURE
*****
NO.   Name                Size      Type      Time
1     main.bin            5988025   N/A      Oct/10/2002 10:10:10
2     backup.bin          5985198   B        Oct/10/2002 10:10:10
3     a.bin               5987491   M        Oct/10/2002 10:10:10
4     s_system.bin        5988022   S        Oct/10/2002 10:10:10
*****
Exit to main menu

```

Press <Enter> to return to the main menu.

4.2.3 Boot Menu 5: Clear the configuration file

Clears the configuration file.

4.2.4 Boot Menu 6: Clear the application program password

Clears the application password.

4.2.5 Boot Menu 7: Ignore configuration file

In this case, an ignore flag will be set in Flash, and the default factory configuration will be used for booting.

Note: The flag is cleaned soon after the system boots.

4.2.6 Boot Menu 8: Enter debugging environment

Enter the debugging environment in case of faults.

4.2.7 Boot Menu 9: Boot ROM Operation Menu

The Boot ROM menu provides two methods for upgrading the program and the Boot ROM sub-menu operations, which are described in the following subsections.

The Boot ROM Operation Option menu includes:

```

Boot ROM Download Menu:
1: Download Boot ROM with XModem
2: Download Extended Segment of Boot ROM with XModem
3: Restore Extended Segment of Boot ROM from FLASH
4: Backup Extended Segment of Boot ROM to FLASH
5: Exit to Main Menu
Enter your choice(1-5):

```

This menu allows you to upgrade, backup, or restore the Boot ROM program.

- Do not check the version of the software

For an upgrade version that is backward compatible with previous releases, do not check the version of the extend segment of the Boot ROM program, Boot ROM program, or the application. If a failure occurs, even if the correct version of the software is used, the software will be regarded as "invalid version". You can select this option to bypass version

checking when upgrading. This option applies only once when selected. When the router is rebooted, version checking is restored.

- Exit and reboot.

Exit the Boot ROM menu and reboot the router.

Note: The Boot menu appears only when you press <Ctrl+B> within 3 seconds after the message "Press Ctrl-B to enter Boot Menu..." appears. If you wish to enter the Boot Menu after the program begins uncompressing, you must to reboot the router.

4.3 Upgrading Software Using Xmodem

You can use the console port to upgrade the software using Xmodem without the need to set up a network environment.

4.3.1 Upgrading the application image

- 1 Enter the Boot Menu (refer to the "Upgrading with FTP" on page 18) and enter <1> to download an application image using Xmodem. The router supports the following downloading speeds:

Please choose your download speed:

- 1: 9600 bps
- 2: 19200 bps
- 3: 38400 bps
- 4: 57600 bps
- 5: 115200 bps
- 6: Exit to Main Menu

Enter your choice(1-6):

- 2 Select an option, 5 for 115200 bps for example. The following appears:

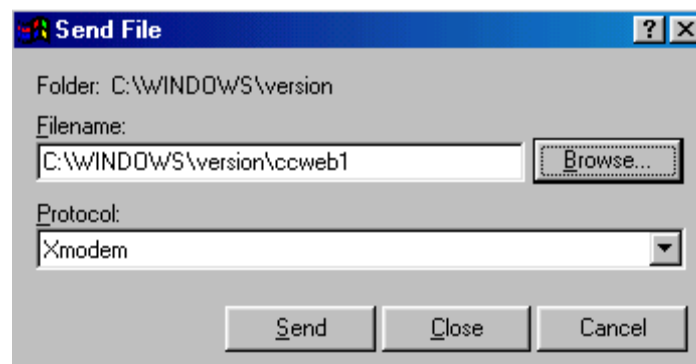
Download speed is 115200 bps. Change the terminal's speed to 115200 bps, and select XModem protocol. Press ENTER key when ready.

- 3 Change your terminal's baud rate to the same baud rate for software download (115200 bps in this example). After that, select [Dial-in/Disconnect] to disconnect the terminal, and [Dial-in/Dialing] to reconnect it. Then, press <Enter> to start downloading. The system displays:

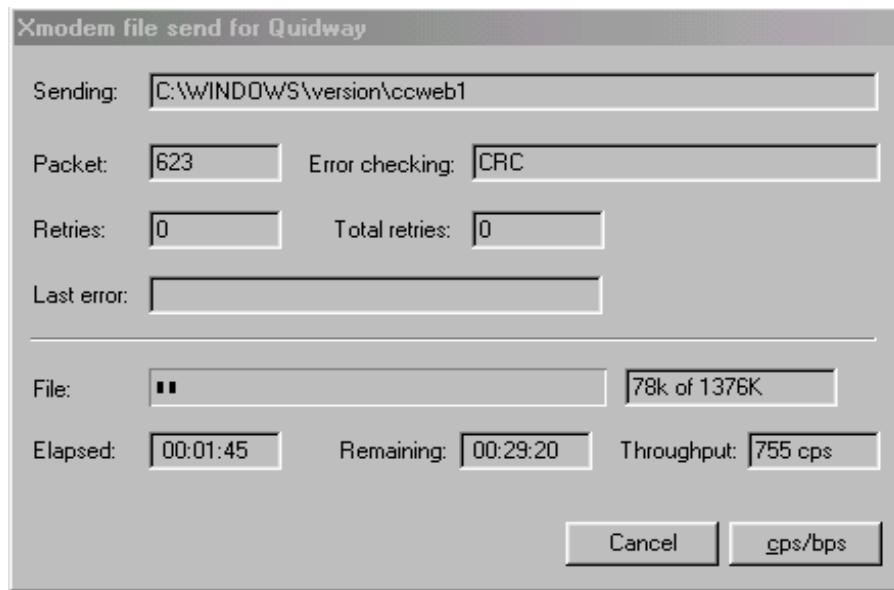
Please Select Program File
Downloading ... CCCCC

Note: The new baud rate takes effect only after you reconnect the terminal emulation program.

- 4 Select [Transfer/Send File] in the terminal window. The following dialog box pops up:



- 5 Click <Browse>. Select the file to be downloaded and set protocol to Xmodem. Click <Send>. The following interface pops up:



The image shows a dialog box titled "Xmodem file send for Quidway". It contains several input fields and buttons. The "Sending:" field is set to "C:\WINDOWS\version\ccweb1". The "Packet:" field is set to "623" and the "Error checking:" field is set to "CRC". The "Retries:" field is set to "0" and the "Total retries:" field is set to "0". The "Last error:" field is empty. Below these fields, there is a "File:" field with a double bar icon and a progress indicator showing "78k of 1376K". At the bottom, there are three fields: "Elapsed:" set to "00:01:45", "Remaining:" set to "00:29:20", and "Throughput:" set to "755 cps". There are two buttons at the bottom right: "Cancel" and "cps/bps".

- 6 After completing the download, the system begins writing data to Flash memory, and then displays the following information on the screen:

Download completed.

The system asks you to select a file type:

please select file to be saved as

1. main application file
2. backup application file
3. secure application file
4. cancel downloading

Enter your choice(1-4):

After you select an option, the system begins writing the file to Flash memory.

Writing to flash memory...

Please waiting,it need a long time (about 5 min).

Write Flash Success.

Please return to 9600 bps. Press ENTER key to reboot the system.

Change the baud rate of the console terminal to 9600 bps, disconnect and re-dial. Then you can see the system boot banner.

4.4 Upgrading Software Using TFTP (option 1)

Use the following procedure to upgrade the software with TFTP:

- 1 You must have level 3 privileges.
- 2 In the User View, enter: `tftp <server ip address or hostname> get <filename>`.
- 3 Enter the System View.
- 4 Set the router to boot from the new image using "boot main <filename>".
- 5 Exit the System View.
- 6 Reboot the router.

The following example illustrates this procedure:

```

<6040>tftp 172.16.1.254 get r6y02_4lvc03.bin
File will be transferred in binary mode. Downloading file from remote
tftp server, please
wait.....
...../ TFTP:
11204734 bytes received in 194 second(s).
File downloaded successfully.
<6040>sys
System View: return to User View with Ctrl+Z.
[6040]boot main r6y02_4lvc03.bin
Set main boot file successfully!
[6040]quit
<6040>reboot

```

4.5 Upgrading Software Using TFTP (option 2)

Upgrading the application image with the NET command will use an Ethernet interface to download. In this approach, the router is the TFTP Client and needs

to connect to a TFTP Server using a fixed Ethernet interface. The following describes how to upgrade the application image with this approach:

- 1 Start the TFTP Server on the host connected to the Ethernet interface on the router. Set the path for the source file to be downloaded.

Caution: No TFTP Server is available on the routers. You must have a TFTP server available.

- 2 In the Boot Menu, select option 2 to enter the Net Port Download Menu (shown below):

```

Net Port Download Menu:
1:  Change Net Parameter
2:  Download From Net to Flash
3:  Download From Net to RAM
4:  Exit to Main Menu
Enter your choice(1-4):1

```

- 3 Select option 1 (Change Net Parameter) to change the download parameters, as shown in the example below.

Note: To modify the parameter values, enter the new values next to the existing values. Do not use the Delete or Backspace key to erase the existing values.

```

Change Boot Parameter:
'.' = clear field; '-' = go to previous field; ^D = quit

boot device           : fei0
processor number      : 0
host name             : 8040
file name             : r5000.bin
inet on ethernet (e) : 10.1.1.110
inet on backplane (b):
host inet (h)         : 10.1.1.241
gateway inet (g)      : 10.1.1.254
user (u)              :
ftp password (pw) (blank = use rsh):
flags (f)             : 0x80
target name (tn)      :
startup script (s)    :
other (o)             :

```

Table 5: Description on the download parameters

Parameter	Description
file name	File name of the router software
inet on Ethernet (e)	IP address of interface eth0.
host inet (h)	IP address of TFTP/FTP Server
gateway inet (g)	IP address of the gateway
user (u)	FTP user name
ftp password (pw)	password used for ftp session
flags (f)	0x80 – TFTP 0x0 -- FTP
target name (tn)	Target file name to be used on the router

- 4 When the Net Port Download Menu is re-displayed, select option 2 (Download from Net to Flash) to download and write the application image to Flash memory. Depending on the running code, the system display would look something like:

```
Net Port Download Menu:
1:  Change Net Parameter
2:  Download From Net To Flash
3:  Download From Net To SDRAM And Run
4:  Upload the current config file to PC
5:  Exit to Main Menu
Enter your choice(1-5): 2
```

```
boot device      : fei
unit number     : 0
processor number : 0
host name       : 8040
file name       : r5000.bin
inet on ethernet (e) : 10.1.1.110
host inet (h)   : 10.1.1.241
gateway inet (g) : 10.1.1.254
flags (f)      : 0x80
```

```
Attached TCP/IP interface to fei0.
Attaching network interface lo0... done.
```

```
Loading...
NET download completed...
read len = [12632583]
```

```
Please select file to be saved as
1. Main application file
2. Backup application file
3. Secure application file
4. Cancel downloading
Enter your choice(1-4): 1
```

```
Creating the file: flash:/r5000.bin
Write data to flash...
```

```
Please wait, it may take a long time!
```

```
#####
#####
#####
#####
```

```
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####
```

Write software file operation success.

Press <Enter> key to reboot the system .